Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Law enforcement access to evidence via direct contact with cloud providers – identifying the contours of a solution

Dan Jerker B. Svantesson [a,b,*], *Lodewijk van Zwieten* [c]

[a] *Faculty of Law, Bond University, Queensland, Australia*
[b] *Faculty of Law, Masaryk University, Brno, Czech Republic*
[c] *Public Prosecutor Specialised in Cybercrime, The Netherlands*

Keywords:
Law enforcement
Electronic evidence
Cloud evidence
Mutual legal assistance (MLA)
Cloud providers
Internet jurisdiction
Provision of data to law enforcement
Evidence
Data storage
Data protection

A B S T R A C T

Effective criminal investigation depends on reliable access to evidence. With the extensive use of cloud computing in various forms, electronic evidence of criminal activity may no longer be found with criminals or their associates themselves. Rather, the evidence resides with cloud providers, oftentimes on servers outside of the territory of the investigating law enforcement authorities (LEAs). Thus, even in otherwise completely domestic criminal investigations of crime committed domestically against a domestic victim, relevant electronic evidence may be stored in a cloud arrangement in another country. Obtaining the evidence in those situations may be difficult.

In this article, we identify 16 variables and a number of fundamental and non-fundamental constraints that must be taken into account by anyone setting out to construct a framework facilitating appropriate LEA access to evidence via direct contact with cloud providers, while safeguarding the rights and interest of individuals, as well as the rights and interest of the provider, and those of other States.

1. Introduction

The ubiquitous use by criminal actors of electronic communications and storage services offered by cloud providers[1] offers various challenges for criminal investigations. Electronic evidence of criminal activity may no longer be found with criminals or their associates themselves. Rather, the evidence resides with cloud providers, oftentimes on servers outside of the territory of the investigating law enforcement authorities (LEAs).[2] The providers holding the evidence may not be incorporated in that territory or have a subsidiary there that acts as a "data controller" and is capable of fully complying with domestic legal process. Obtaining the evidence in those situations in principle requires mutual legal assistance (MLA), although providers incorporated in the US may voluntarily

* *Corresponding author.* Faculty of Law, Bond University, Gold Coast, Queensland 4229, Australia.
E-mail address: Dan_Svantesson@bond.edu.au (D.J.B. Svantesson).

[1] We have opted for the term "cloud provider" so as to avoid linking the discussion to any particular previous definition of the parties concerned. Typically, cloud providers offer services such as infrastructure as a service (IaaS), software as a service (SaaS) and platform as a service (PaaS). For the purpose of this article, we use the term cloud provider to refer to a range of Internet actors, such as providers of social media platforms, email providers and data storage providers, holding user data in cloud arrangements.

[2] For the purpose of this article, LEAs include judicial authorities such as prosecutors and investigating judges.

http://dx.doi.org/10.1016/j.clsr.2016.07.011

disclose non-content data to foreign LEAs on a direct request, without intervention of US authorities.[3]

However, cloud providers with storage facilities in multiple countries may themselves not be able to establish the geographical location of the requested data at any given time, creating uncertainty about the applicable jurisdiction (and with it the lawful application of investigative powers) and possible conflicts of, e.g., data protection legislation.

With regard to voluntary disclosure of non-content data by US-based cloud providers, a coherent, commonly applicable framework does not exist. Providers currently each have their own procedures in place for this type of direct cooperation and make their own assessment of (the legality of) requests in view of fundamental rights and business considerations. This leads to a practice where providers may provide different (subsets of) data in seemingly similar situations, making the process as a whole at times diffuse and unpredictable for requesting LEAs.

In March 2016, the Netherlands organised a conference on the topic of jurisdiction in cyberspace[4]; the topic of direct cooperation with US-based cloud providers was discussed, and it was concluded that "*establishing a clear cooperation framework could benefit States, private sector and its customers as it would increase legal certainty*".[5] In this article we will discuss the relevant considerations that we feel need to be taken into account when devising such a framework.

According to Walden,[6] LEAs seeking access to electronic evidence that is held by a foreign cloud provider typically have four possible courses of action. The LEA may:

(1) seek the assistance of the relevant foreign LEA via formal mutual legal assistance (MLA);
(2) seek informal assistance from the relevant foreign LEA;
(3) seek direct assistance of the foreign cloud provider (that is, without intervention by foreign authorities) or
(4) seek direct access to the data (without third party cooperation).[7]

To this, we would propose to add fifth and sixth possible courses of action. The LEA may:

(5) (spontaneously) share information from the criminal investigation with the foreign LEA, in order to enable them to initiate a domestic investigation – that way, evidence may be acquired domestically, to be subsequently (and spontaneously[8]) shared with the LEA from the original country;
(6) (spontaneously) share information from the criminal investigation with the foreign LEA, which may then investigate and prosecute domestically – this would prevent the need to transfer cloud evidence over borders altogether.[9]

For the purpose of this article, we will focus on option 3: direct cooperation with the foreign cloud provider. Obviously, much can be improved in the current system of MLA,[10] but where such improvements may diminish the need for alternative means of access, it is unlikely that they will eliminate that need altogether. Furthermore, given the fact that substantial changes to the current frameworks which regulate MLA will undoubtedly take a long time to negotiate and effectuate, alternative means of access should, at least for now, be considered to deal with the current challenges of evidence gathering from the cloud. An agreement on alternative means of access could also take some of the current burden of the MLA system, which on its own could improve its functioning. Thus, a discussion on direct cooperation with cloud providers is necessary whether or not we also improve the MLA system as such.

Our aim is to map out the interests and considerations that need to be taken into account in pursuit of a common framework (whatever form it may take), which would regulate the acquisition of evidence via direct contact with (foreign) cloud providers. We do so with the consideration that such cooperation should contain strong safeguards for fundamental rights and personal and legal interests of individuals whose data it concerns, as well as the rights and interest of the cloud

[3] Title 18, paragraph 2702 of the US Federal Criminal Code. This provision was introduced as part of the Electronic Communications Privacy act of 1986 (ECPA), of which the second title was enacted as the Stored Communications Act. Non-content data consists of Basic Subscriber Information (BSI) and transactional data (such as traffic data and connection history), insofar as that data is "at rest". The acquisition of data "in motion" is generally considered a greater infringement on fundamental rights and for that reason requires judicial oversight. In practice, the process of voluntary disclosure of non-content data under ECPA is considerably faster than the MLA process.

[4] "Crossing Borders: Jurisdiction in Cyberspace", 7–8 March 2016, Amsterdam. The conference report (7323/16) can be found at <https://www.parlament.gv.at/PAKT/EU/XXV/EU/09/79/EU_97921/imfname_10617852.pdf>.

[5] Page 10 of the conference report.

[6] Ian Walden, "Law Enforcement Access to Data in Clouds," in Christopher Millard (ed), *Cloud Computing Law* (OUP 2013) 297.

[7] Ibid. As to the option of seeking direct access to the data, this may be sought to be justified by a claim of jurisdiction on various basis, including e.g. on the ground of universal jurisdiction. That option will not be pursued further in this article.

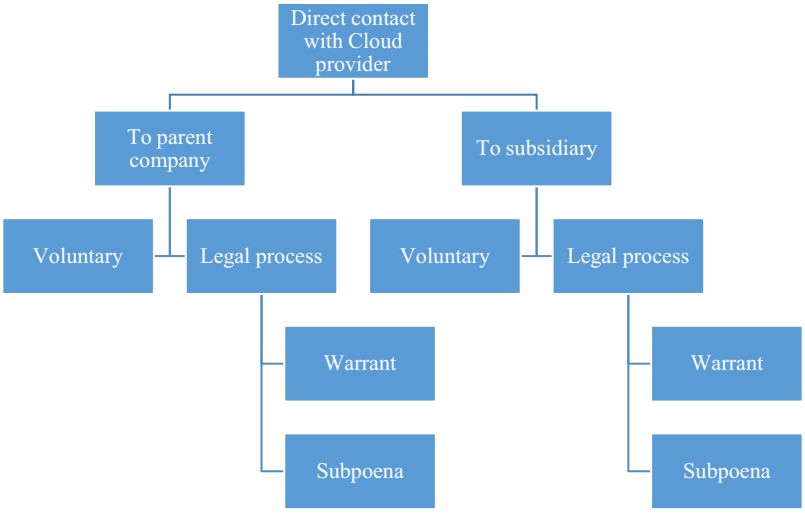
[8] As meant in article 26 of the Council of Europe Convention on Cybercrime (commonly referred to as the Budapest Convention) of 2001.

[9] A formal request to transfer criminal proceedings to the foreign country would fall under option 1 described above.

[10] See: Anna-Maria Osula, "Accessing extraterritorially located data options for States" (2015) <http://english.eu2016.nl/binaries/eu2016-en/documents/publications/2016/03/7/c-osula-accessing-extraterritorially-located-data-options-for-states_anna-maria_osula/c-osula-accessing-extraterritorially-located-data-options-for-states-anna-maria-osula.pdf>; Vivek Krishnamurthy, "Cloudy with a Conflict of Laws" (16 February 2016), Berkman Center Research Publication No. 2016-3 Available at SSRN: <http://ssrn.com/abstract=2733350> or <http://dx.doi.org/10.2139/ssrn.2733350>; Gail Kent, "Sharing Investigation Specific Data with Law Enforcement – An International Approach" (14 February 2014), Stanford Public Law Working Paper <http://ssrn.com/abstract=2472413> or <http://dx.doi.org/10.2139/ssrn.2472413>.

provider and those of other States.[11] Our exercise is not dissimilar to that of Daskal and Woods, but where their approach is explicitly US-centric, our approach is, in essence, jurisdiction neutral.[12] Our mapping exercise is meant to facilitate the discussion on (improved) cooperation between governments and cloud providers. However, we do not weigh these considerations against each other, nor do we propose any order in which they should be addressed.

hand. On a practical level, one may also imagine a third – semi-voluntary – option: LEAs requesting voluntary access with the threat of coercive measures where voluntary access is not provided. In addition, within the category of access through legal process we find different types of instruments such as warrants and subpoenas (typically in the form of production orders or search warrants).



2. The variables and the possible scenarios they create

The task outlined above is not an easy one. And it is made more complex by the fact that situations falling into the third category outlined above are characterised by diversity rather than homogeneity. For example, among the scenarios where LEAs seek the assistance of the foreign cloud provider, we need to (1) distinguish between (typically faster) requests to the parent company and (typically slower) requests that go via domestic subsidiaries.[13] Further, we are also required to (2) distinguish between, on the one hand, access sought on an entirely voluntarily basis, and access based on legal process on the other

These scenarios must be kept separate from situations where LEA seek access to evidence from a domestic cloud provider, such as where a US LEA seeks access to data directly from Microsoft, Google or Facebook. For the purpose of this article we use the term "domestic cloud provider" where the provider is incorporated in the country where the criminal investigation is being conducted, although we do acknowledge that in light of, inter alia, the Yahoo! versus Belgium case[14] and the *Weltimmo*[15] ruling by the European Union's Court of Justice, the prefix "domestic" may be somewhat legally ambiguous in the context of cloud providers.

Regardless of how we define "domestic cloud providers" though, the category as such contains a diversity of possible situations. For example, we could (3) distinguish situations where the data sought relates to a citizen of the State of the

[11] See: Jennifer Daskal & Andrew Keane Woods, "Cross-border data requests: a proposed framework" (2015) <https://lawfareblog.com/cross-border-data-requests-proposed-framework>; Andrew Keane Woods, "A proposal to improve foreign law enforcement access to US-held data" (2015) <https://justsecurity.org/26461/proposal-improve-foreign-law-enforcement-access>; Jennifer Daskal and Andrew Keane Woods, "A new US-UK data sharing treaty?" (2015) <https://www.justsecurity.org/24145/u-s-u-k-data-sharing-treaty>; Jennifer Daskal, "The Microsoft warrant case: the policy issues" (2015) <https://www.justsecurity.org/25901/microsoft-warrant-case-policy-issues>.

[12] Although of course we acknowledge that because of the global dominance of US-incorporated cloud providers, a workable framework is not really imaginable without inclusion of the US perspective.

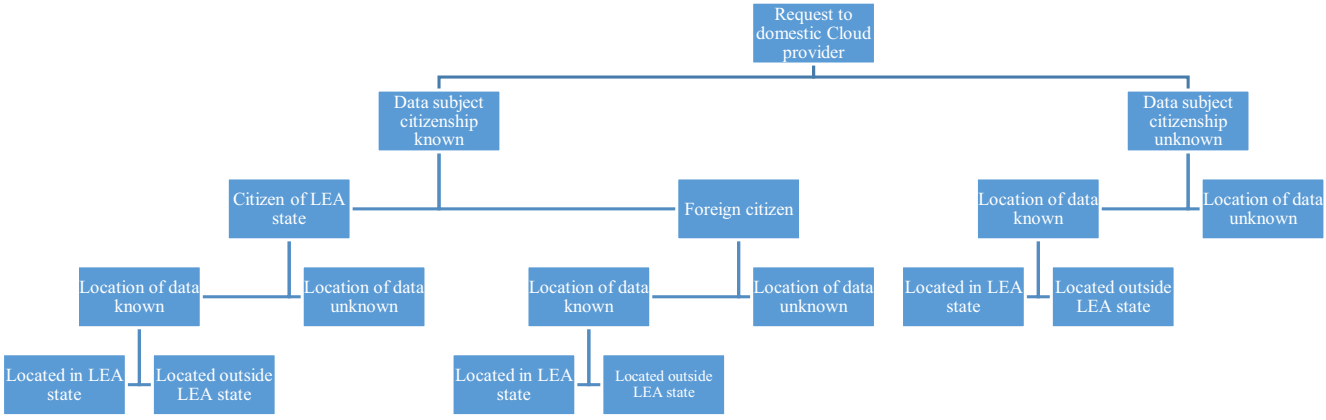
[13] Although exceptions might exist. Typically, requests sent through the subsidiary are assessed by or in coordination with the mother company.

[14] Court de Cassation, 1 December 2015. See: <http://english.eu2016.nl/binaries/eu2016-en/documents/publications/2016/03/7/b-yahoo-court-of-cassation-iii—1-december-2015/b-yahoo-court-of-cassation-iii-1-december-2015.pdf>. An (brief) analysis of the Court's decision can be found at <https://www.stibbe.com/en/news/2016/january/benelux-tmt-cassation-confirms-yahoos-obligation-to-cooperate-with-law-enforcement-agencies>. See also the description of a Danish Supreme Court Order delivered on Thursday 10 May 2012 (Case 129/2011), by Lars Bo Langsted and Helena Lybæk Guƒmundsdóttir, (2013) 10 Digital Evid & Electronic Sig LR 162-5 <http://journals.sas.ac.uk/deeslr/article/view/2038/1975>.

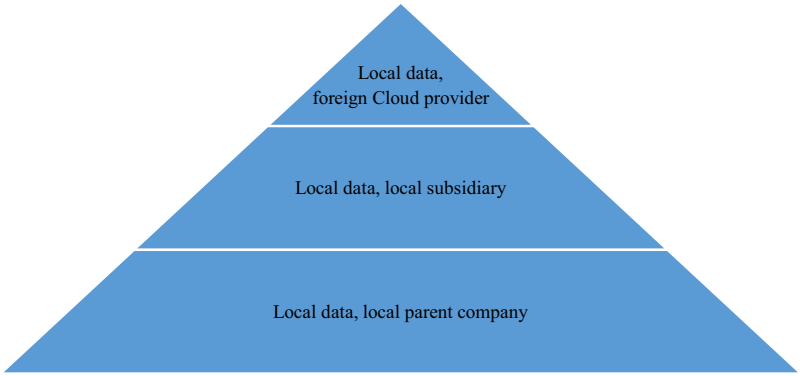
[15] Judgement of 1 October 2015, Case C-230/14). See: <http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d59fb56f2d40734875a7d2a40346901427.e34KaxiLc3qMb40Rch0SaxuTahz0?text=&docid=171574&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=702941>.

investigating LEA from situations where the domestic cloud provider is asked to provide data relating to a foreign national. This distinction is based on the assumption that the citizenship of the data subject is always known. However, when requesting data from a cloud provider, LEAs oftentimes do not (yet) know the nationality of the customer whose information it concerns.[16] This may impede direct cooperation, since cloud providers frequently do factor in the (presumed) nationality of the customer. As a guiding principle for operational processes then, citizenship is perhaps not the most useful.

In the context of data held by the domestic cloud providers, we further (4) distinguish between situations where the data held by the domestic cloud provider is stored domestically (i.e. on a server located in the same country) and situations where the data, while *controlled* by a domestic cloud provider, is *stored* in another country. This is specifically relevant in view of data protection regulations. However, here too we must factor in the possibility of lack of knowledge, in the sense that we need to take account of the fact that the location where the data is held at any given time may be unknown – even to the cloud provider.[17] Furthermore, for some jurisdictions this distinction is legally irrelevant and lawful *control* over the data, irrespective of its geographical location, would suffice to serve coercive legal process under that jurisdiction's domestic laws.



The most complications arise where data is stored locally, but is controlled by a foreign company without a subsidiary in the country of the LEA. Such situations are more complicated than situations where the cloud provider has some corporate presence in that country. By contrast, the easiest situation to deal with is where the data is stored locally and the parent company controlling the data is incorporated within the investigating LEA's territory.



Summarising the above, we have identified six variables that need to be taken into account: (1) the country of the investigating LEA, (2) the country of incorporation of the cloud provider, (3) the existence of subsidiaries in the country of the investigating LEA, (4) the nationality (or habitual residence) of the person to whom the data relates (to the extent ascertainable), (5) the manner in which access is sought (i.e. voluntarily or through legal process) and (6) the location of the data (to the extent ascertainable).

To this, the following variables may be added: (7) the nationality of the suspect(s), (8) the nationality of the victim(s), (9) the location(s) of the suspect(s) at the time of the crime, (10) the location(s) of the victim(s) at the time of the crime, (11) the habitual residence of the suspect(s), (12) the habitual residence of the victim(s) and (13) the availability of alternative means of gaining access to the data, such as via MLA or

[16] Possible identifiers include usernames, IP-addresses, timestamps, language and declared nationality (for instance on a personal page). However, none of those are in themselves a reliable basis to establish the nationality of the subject.

[17] For load balancing purposes and to expedite data retrieval by the customer, data from a single user profile may be stored on servers in multiple jurisdictions at the same time (for instance, BSI and transactional data in the country of incorporation and content data in a storage facility that is geographically close to the location of the customer). This data may be continually in motion.

through direct access by the investigating LEA.[18] Furthermore, in some situations we also need to consider (14) the habitual residence of the witness(es) as well as (15) the location of the witness(es) whose data is sought. In order to construct a framework facilitating appropriate LEA access to evidence via direct contact with cloud providers, this great diversity of variables needs to be taken into account.

3. A proposed method

We have no opinion whether or not the diversity in situations we described above should be reflected in a common framework for direct cooperation with cloud providers. For the purpose of this article, we will focus on certain generally applicable interests and considerations that would at least need to be taken into account when devising a common framework of any sort. To map out these interests and considerations, we will apply parts of a 10-step research method developed and published by Svantesson some years ago.[19] In this research method, the first four steps can be viewed as the analytical phase, with step one defining the problem or research question. Step two seeks to identify any constraints that fundamentally impact on the issue. For example, if one is to find a solution to the regulation of Internet defamation, one cannot ignore the right to free speech – the human right of freedom of expression is therefore a *fundamental constraint*. Step three seeks to identify other, less significant constraints that should be taken into account. We can call them *non-fundamental constraints*. Once all the constraints have been identified, step four is to assess how the constraints interact. For example, some constraints will strengthen each other, while others will be each other's opposites, requiring careful balancing. In this context it must be noted that while certain constraints are fundamental in nature, they may not be *absolute*. In other words, the observation that the right to freedom of expression is a fundamental constraint for any solution to the regulation of Internet defamation does not mean that that right is absolute and may never be limited.

Applied correctly, steps two (the identification of fundamental constraints), three (the identification of non-fundamental constraints) and four (the assessment of how the constraints interact) ensure that the method takes account of the context of the problem that is addressed, thereby disposing of one of the traditional criticisms of stricter doctrinal research methodologies.[20]

The next steps of the research method (steps five to seven) make up the information gathering phase, which is doctrinal in nature and involves an examination of how the problem has been addressed so far (step five), an examination of how similar problems have been addressed so far (step six) and then a critical evaluation of the approaches identified (step seven).

In steps eight, nine and ten (the construction phase), the researcher must construct the solution (step eight) and then test it against the fundamental and non-fundamental constraints (step nine), as well as against any relevant likely future technological developments and uses (step ten). Steps nine and ten work to ensure that the solution serves the purposes it was intended to serve and has the effects it ought to have when put in the context it will operate.

4. The scope of this article

For the purpose of our article we will largely restrict ourselves to steps one, two and three. Thus, our aim is limited and rather modest. However, we envisage that the research model outlined above may fruitfully be applied for the larger task of designing a common framework – whether as a voluntary code of conduct or a binding international agreement – facilitating LEA access to evidence via direct contact with cloud providers. In that sense, what we are doing here can be seen as taking the critical first steps of a longer, indeed much longer, journey. We say critical first steps because they set the direction for all the following steps.

5. Step one – framing the research question

The above has already brought us to the research question. This question may be formulated as: *What considerations must be taken into account in order to create a framework (whichever form it takes) for facilitating lawful LEA access to evidence held by cloud providers, by way of direct contact with those providers, while safeguarding the rights and interest of individuals, as well as the rights and interest of the provider, and those of other States?*

The process of devising such a common framework needs to include a dialogue with a range of parties including governments, cloud providers, LEAs, international organisations with relevant expertise (e.g. the Council of Europe) and academia. The process will likely be difficult and long, but the topic is of such fundamental importance that it should not be put off any longer. This urgency was recently recognised by the Council of Justice Ministers of the European Union, in their recent adoption of conclusions which aim to improve criminal justice in cyberspace.[21]

[18] The Budapest Convention allows such access in certain situations, described in article 32. However, the Convention does not preclude States from legislating other means of direct access. One such example is article 88ter of the Belgian Code of Criminal Procedure, which allows for cross-border preservation of electronic evidence.

[19] Dan Svantesson, "A legal method for solving issues of Internet regulation" (Autumn 2011) 19(3), Intl JL & Info Tech, 243–63.

[20] William Twining, "Academic Law and Legal Development", in *Taylor Lectures 1975* (University of Lagos Faculty of Law 1976) 20, as found in Terry Hutchinson, *Researching and writing in law* (3rd edn, Lawbook 2010) 22.

[21] Conclusions of 9 June 2016 <http://www.consilium.europa.eu/en/press/press-releases/2016/06/09-criminal-activities-cyberspace/>. As part of the Conclusions, the Commission is "requested to develop a common framework for cooperation with service providers for the purpose of obtaining specific categories of data, in particular subscriber data, when allowed by third countries legislation or any other comparable solution that allows for a quick lawful disclosure of such data".

6. Step two – fundamental constraints

The fundamental constraints that step two of the method invites us to identify are constraints of such fundamental importance to the research task defined in step one that a solution that does not take account of them simply cannot be accepted. In other words, *fundamental restraints represent the limits to any acceptable solution*.

The constraints discussed here come in at least three different, but partly overlapping forms. There are practical constraints, such as technical and legal realities, regulatory constraints (such as applicable law that must be taken into account) and aspirational constraints (such as constraints that make reference to societal goals).

We argue that we can identify, at least, 25 such fundamental constraints (discussed below in no particular order and in varying depth), and by mapping them out, we are one step closer to being in a position to start constructing a workable and acceptable framework. Alternatively, for anyone who has already embarked on the journey towards designing a framework facilitating appropriate LEA access to evidence via direct contact with cloud providers, the fundamental constraints outlined here may serve as a useful checklist to assess the work they have done so far.

As was outlined above, currently US-based providers are in a position to provide non-content data on a voluntary basis. Whether a common framework should maintain that basis of voluntary cooperation or replace it with a set of coercive measures is not up to us. Either way, the constraints listed below will be relevant and fundamental.

(1) **Cloud providers have a duty to comply with appropriate legal process, resulting in an obligation to comply with or endure legitimate law enforcement measures.**

This duty is obvious and flows from the rule of law. Also, compliance with legitimate LEA requests could serve corporate interests.[22] The difficulty in the international arena is to identify and delineate which legal obligations apply to a particular cloud provider in any given situation.[23] The strength of the duty to comply is primarily dependent on the degree of connection between the State of the investigating LEA and the State where the cloud has its offices. Domestic legal process does not necessarily compel a cloud provider that is located abroad, unless the authorities of the foreign State transpose such legal process or when legal process is mutually recognised by both the State of the LEA and the State of the cloud provider.[24]

(2) **Cloud providers have a duty to be respectful of the human rights (such as privacy) of their customers.**

This duty flows from a range of human rights treaties, such as the International Covenant on Civil and Political Rights, and in the context of Europe, the European Convention on Human Rights (ECHR) and the Charter of Fundamental Rights of the European Union 2000 which contains a specific right to the protection of personal data. Whereas traditionally the *positive obligation to protect* human rights falls upon governments and not on individuals or corporations, cloud providers nevertheless have a duty to *be respectful* of human rights, such as privacy and protection of personal data.[25] This duty is relevant in assessing whether, and to what degree, to assist LEAs and how to deal with information received by LEAs in search of information held by the provider. However, in practice there is great diversity in how cloud providers factor in basic human rights in their assessment of direct requests. For example, some cloud providers only provide data with regard to IP-addresses that resolve to the territory of the requesting LEA, due to privacy considerations. Other cloud providers do not make this reservation, but they, too, make their considerations based on the right to privacy. It seems then that cloud providers hold different views on how fundamental rights guide their actions in relation to LEA requests.

As said, while rights such as the right to privacy and protection of personal data are fundamental, they are not absolute – in other words, they are constantly subject to balancing exercises involving other, sometimes competing, fundamental human rights.

(3) **Cloud providers have a duty to be respectful of the human rights (such as privacy, protection of personal data and reputation, protection against crime etc.) of non-customers.**

What was said above regarding the duty of cloud providers to be respectful of the human rights of their customers

[22] See generally e.g.: JF Corkery, M Mikalsen, & K Allan, *Corporate social responsibility: The good corporation* (Centre for Commercial Law, Bond University 2015).

[23] We are not just talking about obligations that stem from procedural criminal law, but also from data protection regulation and contractual relations.

[24] Although there are different views on this matter, as is clear from the *Yahoo! v Belgium* ruling. However, for practical reasons, here we will not discuss in depth if the traditional means of enforcing jurisdictional claims in an international context is still feasible in the age of cloud computing.

[25] Horizontal violations of fundamental rights may lead to civil litigation or class actions lawsuits. An example of this are the lawsuits filed against Facebook by Austrian privacy advocate Max Schrems, following the ruling of the Court of Justice of the European Union (CJEU) from 6 October 2015 (ECLI:EU:C:2015:650). In that ruling, the CJEU, inter alia, rendered the Safe Harbour Agreement between the EU and the US invalid. It is interesting to note that, although the right to privacy was a central element in that procedure, the Court was only requested (paragraph 36) to adjudicate the obligation of the competent national data protection authority to investigate a complaint in view of the Charter of Fundamental Rights of the European Union 2000 and the Safe Harbour Agreement. It could be argued that, had the questions referred to the CJEU more expressively concerned the compatibility of the Safe Harbour Agreement with the rights to privacy and protection of personal data (as laid down in articles 7 and 8 of the Charter) or, perhaps more relevant, had the case been brought before the European Court of Human Rights (ECHR), it is entirely possible that the ECHR (with a referral to, inter alia, its ruling in K.U. vs Finland, no. 2872/02, 2 December 2008 and subsequent jurisprudence) would have held Ireland in violation of Mr Schrems' right to privacy (as laid down in article 8 of the ECHR), by not fulfilling its positive obligation to investigate Mr Schrems' legitimate complaint to the Irish Data Protection Commissioner.

also applies here, but the practical considerations of the provider with regard to the response to direct requests from LEAs may be different. This may have to do with the fact that while customers gain some, albeit typically limited, protection from the applicable terms of use, generally no such protection is offered to non-customers.

(4) **Cloud providers cannot comply with conflicting obligations.**

To understand the environment in which cloud providers operate, we may usefully adopt a perspective examining what we can call their "contextual legal system", by which we refer to the system of legal rules that purport to apply to the conduct of the cloud provider in the context of their economic activities.[26] Where a cloud provider is economically active in multiple jurisdictions, that contextual legal system may contain conflicting obligations. This may even prompt the cloud provider to consider wilful non-compliance with the legal obligations of Country A, in order to comply with those of Country B. Such situations are of course unfruitful, harmful and should be avoided. After all, subjectivity to the rule of law should not be an economic consideration but a universally binding principle. Where conflicting obligations cannot be eliminated, the option of providing cloud providers with immunity or other forms of protection (such as so-called "clawback" statutes) should be considered.[27]

At the same time, it should be noted that such conflicts in practice might be less common than what generally is assumed, at least from the perspective of procedural criminal law. First of all, conflicts generally do not arise in MLA situations, since in principle the requested country will have to transpose the foreign judicial order to a domestic one.[28] In those situations, the coercive force exerted on the cloud provider stems from that domestic legal process.[29] A conflict of obligations stemming from criminal procedural law is therefore unlikely. Furthermore, a situation of conflicting obligations would seem logically impossible where disclosure of data is voluntary.

Genuine conflicting duties may arise in scenarios like the ongoing *Microsoft warrant* case,[30] where the cloud provider is simultaneously under a duty to disclose data under the laws of one country (in this case, the US) and (arguably) under a duty not to do so under the laws of another country (in this case, Ireland). These situations will likely only become more prevalent with continuing globalisation. Thus, the concerns are genuine. And until workable solutions have been found for this issue, we cannot really expect the degree of voluntary cooperation from cloud providers to be optimal.[31] Thus, moving forward, it is important that in devising a common framework, domestic legal systems are not viewed independently, but that the focus is on what we refer to as *"jurisdictional interoperability"*, the synergy between different domestic legal systems. To that end, uniting features should be identified and inconsistencies in and clashes of domestic legal systems should be addressed and resolved, both in substantive and procedural law and both from a criminal law perspective as well as from a data protection point of view. Special attention must be given to situations where what is allowed in one country is prohibited or mandatory in another.[32] For example, not all jurisdictions allow for evidence gathering beyond their territory outside of the formal MLA process. Without addressing this issue, these countries would not be able to benefit from any framework that shapes the direct cooperation with foreign cloud providers. This would create an uneven playing field for LEAs and their capacities to effectively and efficiently combat crime. Furthermore, gathering evidence outside of the MLA process could result in admissibility issues regarding the evidence that was received on a direct request. The process of direct requests currently does not contain the same judicial guarantees as the MLA process.[33] A common framework for direct cooperation with cloud providers should address those issues, which may therefore necessitate changes to current domestic and international law.

(5) **The idea of territorial sovereignty as the primary nexus for establishing and enforcing jurisdiction is increasingly at odds with the realities of our interconnected world, which is characterised by constant and fluid cross-border interaction.**

It is already well established that enforcement jurisdiction does not necessarily extend to transitory data in a world where it is increasingly harder to assess when data is truly in motion and when it is at rest.[34] Where the data is in motion, the architecture of the Internet ensures that the shortest and most reliable route is chosen, which is not always a straight line from A to B, meaning that data could

[26] Dan Svantesson, "The holy trinity of legal fictions undermining the application of law to the global Internet" (2015) 23(3) Intl JL & Info Tech, 219-34, 228-30.

[27] Dan Svantesson, "Between a rock and a hard place – an international law perspective of the difficult position of globally active Internet intermediaries" (2014) 30 Computer L & Sec Rev, 348-56.

[28] As remarked upon before, this situation would be different if legal process was mutually recognised in the involved countries.

[29] By coercive force, we mean the obligation to cooperate with or endure legitimate law enforcement measures, in the sense that non-compliance or resistance constitutes a criminal offense.

[30] See: Jennifer Daskal, "The Microsoft warrant case: the policy issues" (2015) <https://www.justsecurity.org/25901/microsoft-warrant-case-policy-issues>.

[31] Of course, if the cloud provider would legally be prohibited to disclose, a request for voluntary cooperation should simply be denied.

[32] Dan Svantesson, "The holy trinity of legal fictions undermining the application of law to the global Internet" (2015) 23(3) Intl JL & Info Tech, 219–234, 234.

[33] The MLA process in principle will allow the judicial authorities of the requesting country to assume that the evidence was gathered by the authorities of the requested country in a lawful fashion. Furthermore, the MLA process forces the requesting country to show that domestic procedures were followed and that the request is made by the appropriate authority.

[34] For instance, for the purpose of cloud services, load-balancing configurations may require account data to be transferred regularly without active user involvement. A data transfer therefore does not necessarily constitute a "communication" in the traditional, legal sense of the word.

cross many jurisdictions. Furthermore, cloud providers may store their customers' data in or close to the territory where their customers reside for business reasons,[35] to allow for fast access to that data by the user (caching or mirroring), thereby enhancing the user experience. Similarly, users of specific cloud communication services may choose to use that specific service because of many reasons (low cost, peer pressure, aesthetics, etc.), but usually a deliberate decision to seek the protection of the legislation of the jurisdiction where the provider is incorporated is not one of them. From the above, it is clear that the presence of (certain types of) data in a certain territory at any given time is either a result of the business model of the cloud provider or a *technical coincidence*, but in any case, often outside of the influence of the customer.

However, for the purpose of criminal investigations or the protection of the domestic legal order, territoriality is a (still) primary guiding principle. We are of course not discounting that principle as a whole, but it needs to be pointed out that the Internet and cloud computing surely have tested this principle to its limits, leading in certain cases to undesirable or even absurd situations. For instance, LEAs are encountering more and more instances where hosting services are being *off-shored*. In the country where the criminal investigation is conducted, it may be established that the evidence is located on a server within that territory, but access to that data may require information that is held by a reseller in another country, prompting a need for mutual legal assistance. Another example is the, somewhat disturbing, trend in courts from around the world ordering the global deletion of content violating local law, where no concerns appear to be raised about the fact that deleting that content on servers outside of the court's territory may interfere with the sovereignty of foreign States.

In our hyperconnected world, the idea that the State ipso facto has (exclusive) jurisdiction over all data that is stored within or that passes its territory is simply not sustainable. While territorial thinking is binary – either something happens on a State's territory or it does not – the legitimacy of jurisdictional claims certainly should not be; there is always a matter of degree. After all, legitimacy in essence is a matter of "accepted authority", the establishment of which should include a visible weighing of (possibly opposing) interests involved. If we are to make progress in the matter of LEA access to evidence via direct contact with cloud providers, we need to change our paradigm. We should perhaps abandon the territoriality principle as the core of our thinking on jurisdiction and replace it with a test that better reflects the realities of why data is where. Of course sovereignty considerations should be a part of this new paradigm – after all, there still *are* borders in the physical world, but the scope would be broader.

We here propose that such a test includes the notion of *investigative jurisdiction*[36] as introduced by Svantesson. The essence of that notion is as follows:

In the absence of an obligation under international law to exercise jurisdiction, a State may only exercise jurisdiction where:

(1) *there is a substantial connection between the matter and the State seeking to exercise jurisdiction;*
(2) *the State seeking to exercise jurisdiction has a legitimate interest in the matter; and*
(3) *the exercise of jurisdiction is reasonable, given the balance between the State's legitimate interests and other interests.*[37]

An important consequence of the observation that the legitimacy of any given jurisdictional claim is a matter of degree, is that it is possible to imagine a gradual system where the type and detail of data that is provided to a LEA depended on the strength of the legitimacy of the jurisdictional claim. Under such a system, where a LEA can show a strong legitimacy of its jurisdictional claim, detailed and extensive data may be provided to that LEA, while where a LEA can show only an adequate, but comparatively weak, basis of its jurisdictional claim, only limited data may be provided to that LEA.

(6) **In approaching the question of jurisdiction, investigative measures cannot be adequately handled under the strict rules governing enforcement jurisdiction.**

International law typically distinguishes between three types of jurisdiction: prescriptive jurisdiction, judicial jurisdiction and enforcement jurisdiction. A key reason for the current difficulties associated with LEA access to evidence via direct contact with cloud providers is found in the fact that such investigative measures fall into the category of enforcement jurisdiction – the type of jurisdiction most tightly bound up by the territoriality principle. However, criminal investigations in the cloud test this principle to its fundamental and practical limits. Two examples may illustrate this.

Imagine that State A sends an LEA into State B to arrest a citizen of State B, in order to bring him before a court in State A. The legitimacy of that action is dependent on State A having enforcement jurisdiction (i.e. if its enforcement jurisdiction extended to the territory of State B).[38] Now imagine that LEA in State A, within its territory, has lawfully gained access to a laptop belonging to a citizen of State A. When they examine that laptop, they find that relevant files are stored locally on the laptop while others are stored

[35] Unless, of course, they are obliged by law to store the data within a certain geographical location. However, such data localisation requirements for the purpose of protection of personal data and privacy are fairly recent whereas caching and mirroring are long-standing business practices.

[36] Dan Svantesson, "The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Businesses" (2014) 50(1), Stan J Intl L, 53–102.

[37] See further: Dan Svantesson, "A New Jurisprudential Framework for Jurisdiction: Beyond the Harvard Draft" (2015) 109, Am J Intl L, Unbound 69 <https://www.asil.org/blogs/new-jurisprudential-framework-jurisdiction-beyond-harvard-draft> accessed 9 April 2016. This approach to jurisdiction has been endorsed in the Netherlands Presidency of the Council of the EU Debriefing Conference on Jurisdiction in cyberspace (7–8 March 2016, Amsterdam) doc. 7323/16.

[38] Likely, the actions of State A would not pass that test, without a basis in international law or an explicit consent of State B. Moreover, the "arrest" would likely be perceived as a criminal offence by State B.

in on servers in State B. The legitimacy of accessing that remotely stored data, although dramatically different to the first situation, would also be dependent of State A having enforcement jurisdiction, but the outcome of that assessment is arguably much more unambiguous than in the first example and highlights a need for increased sophistication in the categorisation of various jurisdictional claims under public international law.

To make progress we need to recognise that LEA access to evidence via direct contact with cloud providers may actually fall into a previously overlooked fourth category of jurisdiction – what we call *investigative jurisdiction* (see above) that can be somewhat more practical in its relationship to territoriality.

(7) **Where a cloud provider enjoys rights in a State where it has a corporate presence and where that State has a legitimate interest in the cloud provider, those rights and interests must be considered when an assessment is made as to whether the cloud provider should comply with duties, conflicting with those rights and interests, stemming from another country.**

The relevance of those rights is a matter of degree where the level of substantial connection and legitimate interest must be considered. For example, in the absence of other connecting factors and interest, the State of incorporation may enjoy a stronger interest in, and connection to, the cloud provider than does the State where the data happens to sit on a server. However, this balance may quickly change if other connecting factors and interests point to an overall more substantial connection to, and legitimate interest of, the State where the data sits. In other words, a careful case-by-case balancing is required.

(8) **Different rules are needed for different types of data as the degree of data privacy sensitivity varies.**

This distinction cannot solely rely on the binary distinction between personal data and non-personal data, which is typical of data protection laws. Neither should this distinction solely be based on the differentiation between subscriber data, transactional data (including traffic data) and content data (or the even more inelegant distinction between metadata and data), since the sensitivity of the data would depend on the service to which the information relates, the amount of data[39] and its intended use. Thus, while distinctions such as those outlined above are common in domestic law as well as in international instruments, we might need more sophisticated delineations that better correspond to the actual privacy implications of the data that is being disclosed.

Such a distinction is also relevant in view of the extent to which disclosure of data should be left to the discretion of cloud providers. As said, currently voluntary disclosure by US-based cloud providers is limited to non-content data. Disclosure of content data would typically constitute a greater infringement on the privacy of the user(s) in question. In many countries, this greater impact on privacy is reflected in a requirement of judicial oversight for the acquisition of communication content. It may be argued that private entities should perhaps not be encouraged to adjudicate the merits of a case in a fashion that under other circumstances would be the prerogative of judicial authorities. A common framework for direct cooperation should therefore include reflections on the quasi-judicial nature of the assessment by cloud providers in view of the extent of the privacy implications of voluntary disclosures (see also fundamental constraints 2 and 3 above).

(9) **A distinction between access to stored (historical) data and live data is necessary.**

The difference between access to stored data and access to live data – or perhaps more elegantly, "data at rest and data in motion" – is well established and must be recognised in the discussions.

(10) **Digital evidence stored on foreign servers is frequently relevant in relation to completely domestic crimes.**

The way people use information technology has resulted in a situation where evidence frequently is stored in foreign jurisdictions even though the criminal activity in question is entirely domestic – a local offender, a local act and a local victim. Imagine for instance a situation where person A is a drug dealer from Amsterdam. He imports his drugs by boat. At the seaport in Rotterdam (also in the Netherlands), he has several security officers on his payroll, enabling him to clear the containers that contain the drugs without inspection. In a criminal investigation into A's dealings, the police find out he communicates with his security officers at the seaport through a Gmail account.

Now, if the police want to obtain information from Google, they would have to send a request to Google's offices in the US or their subsidiary in Ireland, or they would have to send an MLA request to the American or Irish authorities. This is somewhat strange, since the crime is committed on Dutch soil and all the perpetrators are Dutch as well. The only US nexus is the cloud mail service that is being used. But as we saw above, in the bulk of these situations, the fact that (part of) the data is stored abroad is likely a technical coincidence. To make things worse, the legal threshold to acquire content data under US law (the probable cause requirement) is higher than the threshold that needs to be met under Dutch law. All in all, having to resort to international cooperation instruments in a situation of a strictly domestic crime can be a serious impediment to effective criminal investigations and be very frustrating to boot.[40]

[39] For instance, basic subscriber information relating to an LGBT communication platform would reveal information about sexual orientation, which is highly privacy sensitive. Similarly, analysis of transactional data that covers a prolonged period of time could yield a more or less complete picture of certain aspects of the personal life of the person whose information it concerns (and perhaps a greater invasion of privacy than was foreseen under the original request).

[40] A possible way forward could be to have the domestic legal requirements of the requesting country be the guiding principle for the execution of requests for data in cases where the crime and all its actors are local and the presence of data in the requested country is merely a technical coincidence. Such a provision could prevent the need to transpose foreign judicial orders altogether and would be very similar to a situation of direct recognition or the European Investigation Order.

(11) **Where fully respected, anonymity – an articulated component of some data protection frameworks – undermines the identification of factors such as the relevant person's location, nationality and residence.**
Any framework facilitating LEA access to evidence via direct contact with cloud providers must carefully balance the legitimate calls for anonymous interaction online with other relevant (and likely competing) interests.

(12) **Cloud providers must be transparent as to how many requests for access they get, from where those requests originate, what those requests relate to, how many requests result in access being granted, etc.**
Several major cloud providers already issue "transparency reports" outlining this type of information. The reverse is also possible: in the US, the Attorney General, according to 18 USC §2702 is obligated to report to the House of Representatives and the Senate on the number of voluntary disclosures by cloud providers. Obviously any disclosure of information about voluntary cooperation, regardless of who does the reporting, must be carefully presented so as to not reveal personal data or interfere with ongoing criminal investigations.

(13) **Cloud providers need to be transparent in their terms of use as to how they interact with LEAs, including how they treat the information they receive as part of data requests.**
Transparency is needed, for example, as to when data is voluntarily disclosed, when disclosed upon request, when disclosed under a court order etc. To a degree, but only to a degree, user expectations can be managed this way. However, we must be mindful that users rarely read and understand the terms of use – truly informed consent is somewhat of a fairy tale concept. In addition to these resources, we must ensure that any framework contains mechanisms to control how cloud providers treat the – sometimes very sensitive – data they are provided as part of the request. For example, we want to avoid a situation where cloud service users receive targeted advertisement for lawyers specialising in particular fields corresponding to the request cloud providers receive from LEAs.

(14) **Cloud providers need to be transparent in informing the affected user where data is in fact communicated to LEAs, unless there are strong reasons not to inform the user.**
In identifying when a user should not be informed, we can draw upon existing legislation and practices addressing this matter.

(15) **The urgency of data access will vary from case to case.**
Emergency access procedures must be put in place for certain clearly defined and delineated situations. There are obvious precedents to build on in this context, and many cloud providers already have an emergency disclosure procedure in place.

(16) **Individuals have an interest in their data protection rights.**
As is clear from international human rights law, these rights are fundamental but not absolute (as in unrestricted). We will not enter here into a detailed consideration of exactly what those rights are and only stress that that data protection is both a fundamental right for its own sake and an enabling right catering for the enjoyment of other fundamental human rights such as freedom of expression and the right to privacy. Undue limitations of the right to data protection (for instance, due to mass surveillance) or insufficient protection of this right by governments (for instance by not setting standards for data protection) are likely to have a chilling effect on the exercise of these other rights.

(17) **Individuals have a general interest in crimes being detected, investigated and prevented and in criminal justice being served.**
This interest is rooted in the proper functioning of society and exists irrespective of the location from which the crime was committed and irrespective of the location where evidence necessary to investigate and prosecute may be found.

(18) **Victims of crime have a particular interest in crimes being detected, investigated and prevented and in criminal justice being served.**
This interest exists irrespective of the location from which the crime was committed and irrespective of the location where evidence necessary to investigate and prosecute may be found.

(19) **States have a duty to be good world citizens so as to help legitimate law enforcement actions in other countries.**
The strength of this duty is partly dependent on the type of crime (e.g. child abuse should concern everyone) and on the international legal instruments that exist to foster cooperation between States.

(20) **States have a duty to act against criminal activities within their jurisdiction so as to prevent those criminal activities affecting other States or their citizens.**
This duty is a necessity in the international system, not least in order to avoid "safe havens".

(21) **States have a duty to be respectful of and to protect human rights (such as the right to privacy, data protection, etc.).**
Again, this indisputable duty is founded on international human rights law.

(22) **It is not always possible to ascertain the geographical location of the server on which data resides.**
At least currently, it is not always feasible to ascertain the geographical location *with reasonable effort* and *within a reasonable time*. In those situations, even if an extensive search on a deep technical level might eventually establish the geographical location, for the purpose of effective criminal investigations and prosecutions the location may be assumed to be "unknown". This is in contrast to the current rules where the location of the data is a determining factor in the assessment of whether LEAs lawfully have access to the data.

(23) **In the context of cloud computing, data is frequently distributed over more than one server, either as duplicates or simply by the fact that it is broken into small parts.**
As a result, data regarding the profile of a single user may be stored in different jurisdictions simultaneously. This is an effective and desirable structure, but it is in contrast to the current rules where the location of the data is a determining factor in the assessment of whether LEAs lawfully have access to the data.

(24) **Appropriate procedural safeguards ensuring legitimacy of data request must be established.**
Such procedural safeguards cannot merely refer to vague references to human rights standards as these standards are neither sufficiently clearly defined nor universally agreed upon. Rather, what amounts to appropriate procedural safeguards in the context of LEA access to evidence via direct contact with cloud providers must be identified in detail.

(25) **The proper substantive rules, scope, structure and nature of any framework for facilitating lawful LEA access to evidence via direct contact with cloud providers will need to reflect the differences in the legal traditions of the countries covered by the framework, but with a minimum standard to be met.**
Substantive and procedural law may bring with them different requirements regarding the type of information required to meet the burden of proof, the chain of custody and the presentation of evidence in court. A common framework will need to reflect those differences. At the same time, there are countries that have different attitudes towards matters such as human rights and due process. In light of this, it may be that a framework for facilitating lawful LEA access to evidence via direct contact with cloud providers should not (yet) be open to all countries. Thus, while we must aim to make our solutions of today scalable to the world of tomorrow, where hopefully many more countries can join the framework, we do not need to try to construct a solution that caters for request from countries failing to meet appropriate human rights and due process standards.

As we said before, all these 25 fundamental constraints must be taken into account when designing a common framework for facilitating appropriate LEA access to evidence via direct contact with cloud providers.

7. Step three – non-fundamental constraints

For step three, we will identify the relevant non-fundamental constraints, but we will not discuss them in depth. Like the fundamental constraints, the non-fundamental constraints come in at least three different forms: practical constraints, regulatory constraints and aspirational constraints. They are as follows:

(1) It is easier to build on existing instruments (e.g. the Council of Europe's Budapest Convention on Cybercrime) than it is to build an entirely new solution;
(2) Initial consensus is best sought within a group of countries with broadly similar legal traditions and with a certain degree of trust in LEA cooperation. The EU is an obvious candidate in light of its relative existing harmonisation (and given that many of the relevant data protection constraints will stem from the EU);
(3) Rules for LEAs should meet principles of transparency and accountability and should therefore be separate from rules for intelligence services. At the same time, the reality is of course that in areas such as corporate espionage and terrorism, it is not always easy to draw sharp lines between LEA activities and the activities of intelligence services;
(4) Balkanization incurs a cost, a financial cost for intermediaries, and at least an efficiency loss for users;
(5) While perhaps unsurprising in the current climate, unilateral extension of domestic territorial jurisdiction by allowing LEAs to gain direct access to data held by cloud providers is unsuitable as a long-term strategy;
(6) The efficiency of the actual cooperation between LEAs and intermediaries will always and to a great degree, depend on the extent to which a "culture of cooperation" exists or can be developed;
(7) Harmonisation of substantive law, while useful, is not likely in the short term, and thus procedural laws must be coordinated;
(8) It would be appropriate to include limitations as to what type of crimes will be covered by the framework, allowing LEA access to evidence via direct contact with cloud providers. First, from a practical perspective, this will likely help limit the number of requests. Second, given the privacy concerns involved, perhaps not all crimes are of such importance as to legitimise the voluntary disclosure of privacy sensitive data. In any case, possibilities to disclose information voluntarily should be limited, in view of data protection and privacy concerns;
(9) Where a cloud provider hands over data to a LEA, that process incurs a cost. One matter to be considered is who should carry that cost; and
(10) The manner in which information is acquired may impact its admissibility or reliability when presented as evidence in courts.

8. Concluding remarks

In this article, we have pointed to 16 variables and a number of fundamental and non-fundamental constraints that anyone setting out to construct a framework facilitating appropriate LEA access to evidence via direct contact with cloud providers must take into account, either by making sure that their proposed frameworks actually cater for the rich diversity of scenarios those variables make possible or by adopting limitations narrowing the scope of their proposed frameworks.

As should be clear from the above, the matter discussed here is complex and necessitates the balancing of a range of important considerations. And as also ought to be clear, it is not an area that lends itself to simple – one-dimensional – solutions. In light of this, we do not believe it will be possible to identify any single 'connecting factor', the application of which will always result in legitimate LEA access to evidence held by cloud providers, by way of direct contact with those providers, while safeguarding the rights and interest of individuals, as well as the rights and interest of the provider, and those of other States. Interest balancing is the key.

At the same time, we are conscious that any framework (whichever form it takes) for facilitating lawful LEA access to evidence held by cloud providers, must be clear enough to be applied with ease at least in standard situations.

At any rate, it is perhaps unsurprising that civil rights activists and LEAs view the discussed matters from different

perspectives. And it is perhaps equally unsurprising that there also are great cultural differences between the US and Europe in how various stakeholders view the relevant considerations and how these considerations should be balanced. This seems to have resulted in a disconnect between the various initiatives taken in this arena in Europe and the US. If a solution with potential for long-term success is to be found, we necessarily must map out and agree upon what are the relevant considerations. The above has all been aimed at this first step.

If the fundamental constraints outlined above are accepted as an appropriate description of these considerations, stakeholders should proceed to enter into a dialogue as to how these considerations ought to be balanced; because one thing is certain, insisting on absolute privacy protection or unfettered LEA access to data will get us nowhere. And if we fail to find appropriately balanced solutions, we should not expect a *status quo* to be maintained. As said, unilateral solutions to extend enforcement jurisdiction outside of the territorial borders are not sustainable in the long term.[41] Given the urgency of the problem however, that practice is likely to increase rather than decrease.

Acknowledgements

In writing this paper, we have benefitted greatly from speaking, and getting feedback, at Crossing Borders: Jurisdiction in cyberspace, Dutch EU Council Presidency (The Netherlands) (March 2016) as well as at the "Jurisdiction and Extraterritoriality in a Connected World" session at RightsCon in San Francisco (March 2016). We also thank Mark Zoetekouw for his detailed feedback, as well as a large number of other colleagues who have provided valuable comments on earlier drafts of this article.

Professor Svantesson is a recipient of an Australian Research Council Future Fellowship (project number FT120100583). The views expressed herein are those of the authors and are not necessarily those of the Australian Research Council.

REFERENCES

Yahoo! v *Belgium*, Belgium Supreme Court decision, <http://english.eu2016.nl/binaries/eu2016-en/documents/publications/2016/03/7/b-yahoo-court-of-cassation-iii—1-december-2015/b-yahoo-court-of-cassation-iii-1-december-2015.pdf>; 1 December 2015.

Corkery JF, Mikalsen M, Allan K. Corporate social responsibility: the good corporation. Centre for Commercial Law, Bond University; 2015.

Danish Supreme Court Order delivered on Thursday 10 May 2012 (Case 129/2011).

Daskal J. The Microsoft warrant case: the policy issues, <https://www.justsecurity.org/25901/microsoft-warrant-case-policy-issues>; 2015.

Daskal J, Woods AK. Cross-border data requests: a proposed framework, <https://lawfareblog.com/cross-border-data-requests-proposed-framework>; 2015a.

Daskal J, Woods AK. A new US-UK data sharing treaty?, <https://www.justsecurity.org/24145/u-s-u-k-data-sharing-treaty>; 2015b.

Kent G. Sharing investigation specific data with law enforcement – An international approach, Stanford Public Law Working Paper <http://ssrn.com/abstract=2472413> or <http://dx.doi.org/10.2139/ssrn.2472413>; 2014.

Krishnamurthy V. Cloudy with a conflict of laws, Berkman Center Research Publication No. 2016-3, <http://ssrn.com/abstract=2733350> or <http://dx.doi.org/10.2139/ssrn.2733350>; 2016.

Langsted L, Lybæk Guƒmundsdóttir H. Case Translation, 10 Digital Evid & Electronic Sig LR 162-5, <http://journals.sas.ac.uk/deeslr/article/view/2038/1975>; 2013.

Netherlands Presidency of the Council of the EU. Crossing borders: jurisdiction in cyberspace, conference report, <https://www.parlament.gv.at/PAKT/EU/XXV/EU/09/79/EU_97921/imfname_10617852.pdf>; 2013.

Osula A. Accessing extraterritorially located data options for States, <http://english.eu2016.nl/binaries/eu2016-en/documents/publications/2016/03/7/c-osula-accessing-extraterritorially-located-data-options-for-states_anna-maria_osula/c-osula-accessing-extraterritorially-located-data-options-for-states-anna-maria-osula.pdf>; 2016.

Svantesson D. A legal method for solving issues of Internet regulation. Int J Law Info Tech 2011;19(3):243.

Svantesson D. Between a rock and a hard place – an international law perspective of the difficult position of globally active Internet intermediaries. Comput Law Secur Rep 2014a;30.

Svantesson D. The extraterritoriality of EU data privacy law – its theoretical justification and its practical effect on U.S. businesses. Stanford J Int Law 2014b;50(1):53–102.

Svantesson D. A new jurisprudential framework for jurisdiction: beyond the Harvard draft. AJIL Unbound 2015a;109:69. <https://www.asil.org/blogs/new-jurisprudential-framework-jurisdiction-beyond-harvard-draft>.

Svantesson D. The holy trinity of legal fictions undermining the application of law to the global Internet. Int J Law Info Tech 2015b;23(3):219–34.

Twining W. Academic law and legal development. In: Taylor lectures 1975 (University of Lagos Faculty of Law 1976) 20, as found in Terry Hutchinson. 3rd ed. Researching and writing in law. Lawbook 2010 22.

Walden I. Law enforcement access to data in clouds. In: Millard C, editor. Cloud computing law. OUP; 2013.

Woods AK. A proposal to improve foreign law enforcement access to US-held data, <https://justsecurity.org/26461/proposal-improve-foreign-law-enforcement-access>; 2015.

Dan Jerker B. Svantesson – Professor and Co-Director, Centre for Commercial Law, Faculty of Law, Bond University (Australia). Visiting Professor, Faculty of Law, Masaryk University (Czech Republic). Researcher, Swedish Law & Informatics Research Institute, Stockholm University (Sweden).

Lodewijk van Zwieten – Public prosecutor specialising in cybercrime, The Netherlands. l.j.a.van.zwieten@om.nl.

[41] See the *Yahoo! v Belgium* case.